RECEIVED
CENTRAL FAX CENTER
JUL 06 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Maino, et al.

Attorney Docket No.: ANDIP004

Application No.: 10/034,367

Examiner: TESLOVICH, TAMARA

Filed: December 27, 2001

Group: 2137

Title: METHODS AND APPARATUS FOR SECURITY OVER FIBRE CHANNEL

CERTIFICATE OF FACSIMILE TRANSMISSION:
I hereby certify that this correspondence is being transmitted by facsimile to the United States Patent and Trademark Office, Commissioner for Patents, Attn: Examiner Teslovich, Fax No. 571-273-8300, Alexandria, VA 22313-1450 on: July 6, 2006

Signed: _____
Joyce L. Ferreira

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant requests review of the final rejection in the above-identified application. No 10/034,367, no amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reasons stated on the attached sheets.

Remarks begin on page 2 of this paper.

Attached is an appendix of claims.

JUL 0 6 2006

REMARKS

Claims 1-25 were withdrawn from consideration. Claims 26-50 were rejected under 35 U.S.C. 102(e) as being anticipated by Hagerman (USP 6,973,568).

Hagerman describes a storage area network resistant to spoofing and replay attacks. Hagerman details authentication using a hash function. "Each port is provided with a hash function generator for providing and verifying an authentication code for frames transmitted over the storage area network, and a key table for providing a key to the hash function generator. The authentication code is generated by applying a hash function to the key and to at least an address portion of each frame. In each node, the key is selected from that node's key table according to address information of the frame." (Abstract) "Fibre Channel storage area network utilizes frames having time-of-transmission and authentication-code fields." (Column 3, Lines 23-24) "The Authentication code field 300 is filled with a hash function of at least a key value, the transmitted time field 302, the S—ID field 304, the D—ID field 306, and any association header field 308. The hash function that generates authentication code field 300 may also operate upon additional fields of the header and payload, security is enhanced by including the payload 310. It is preferable that the hash function be computed by hardware associated with each port, such as hash function generators 182, 184, 186, 188, 190, and 192 (FIG. 1). Software hash function generators may consume considerable compute resources. The key value used to compute the authentication code field 300 is extracted from a key table 170, 172, 174, 176, 178, and 180 associated with each port." (Column 5, Lines 15-28) "The authentication code is computed using the MD2 hashing algorithm." (Column 3, Lines 41-42)

"Each node that receives the transmitted frame recomputes the authentication code based upon a key selected from the table according to the S—ID of the frame header. The recomputed authentication code is compared to that in the frame, those frames having mismatched authentication codes are dropped." (Column 3, Lines 48-53)

Hagerman is believed to teach or suggest only conventional fibre channel security. "In conventional implementations, no security is provided in the initialization messages. The techniques of the present invention provide mechanisms for embedding security in the

initialization messages to create an initialization sequence with security... techniques are also provided for authentication between non-adjacent entities." (Page 9, Line 28 – Page 10, Line 4)

Independent claim 26 recites "identifying a security control indicator in the frame." Claim 50 similarly recites "means for identifying that the frame has been secured." Claims 36 and 46 have been amended to recite "providing a security control indicator in the fibre channel frame, wherein the security control indicator specifies that the fibre channel frame is encrypted." The material the Examiner cites does not teach or suggest any security control indicator. The Examiner argues that an authentication code field is a security control indicator and cites column 5, lines 15-41. "The Authentication code field 300 is filled with a hash function of at least a key value, the transmitted time field 302, the SID field 304, the DID field 306, and any association header field 308. The hash function that generates authentication code field 300 may also operate upon additional fields of the header and payload, security is enhanced by including the payload 310. It is preferable that the hash function be computed by hardware associated with each port, such as hash function generators 182, 184, 186, 188, 190, and 192 (FIG. 1). Software hash function generators may consume considerable compute resources." (Column 5, Lines 15-41).

The authentication code field in Hagerman is merely the output of a hash function. The hash function may have been applied to different fields, such as a key value, transmitted time, SID, and/or DID, but authentication code field still only holds the output of a hash function. The output of a hash function or any hashed field is not a security control indicator.

The security control indicator is used to indicate whether a frame supports security so that either conventional frame processing or modified frame processing can be used. "The header can also include a security control indicator . . . bit showing that the frame should be decrypted and authenticated." (page 17, lines 28-29) "In one example the security control indicator is set by changing a vendor specific value." (page 19, lines 15-16)

Hagerman has no indicator showing whether a frame is secure. An authentication code is provided in every frame and thus Hagerman has no need to provide a security control indicator. Furthermore, even if the authentication code in Hagerman is interpreted broadly as a security control indicator, the authentication code does not to indicate any encryption support associated with the frame. Cryptography includes both encryption and authentication. Hagerman deals only with authentication. The hash value in Hagerman does not indicate if a

frame should be decrypted. Hagerman does mention encryption in column 7, lines 27-34. "These packets are received at a second firewall 622 where they are decrypted and de-encapsulated for transmission over the second SAN segment 608 to receiving port 606." Without further detail, Hagerman seems to suggest that all frames are decrypted and deencapsulated. This suggests that there is no need again for a security control indicator.

Independent claim 26 also recites "determining that a security association identifier associated with the frame corresponds to an entry in a security database." Hagerman does not teach or suggest determining that any security association identifier corresponds to an entry in a security database. In fact Hagerman, does not even describe a security association identifier.

Independent claim 26 also recites "decrypting the first portion of the frame by using algorithm information contained in the entry in the security database." Independent claim 50 also recites "means to decrypt the eventually encrypted frame." The material the Examiner cites only describes calculating an authentication code. Calculating an authentication includes performing authentication or hashing operations that are distinct from performing code decryption operations. Other independent claims also recite encrypting or decrypting using information associated with a security database. Hagerman does not teach or suggest encrypting or decrypting using any information associated with a security database.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Godfrey K. Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100

Appendix – Independent Claims

26. (Original) A method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a frame at a first network entity from the second network entity in a fibre channel network;

identifying a security control indicator in the frame from the second network entity;

determining that a security association identifier associated with the frame corresponds to an entry in a security database;

decrypting the first portion of the frame by using algorithm information contained in the entry in the security database.

36. (Previously Presented) A method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

providing a security control indicator in the fibre channel frame, wherein the security control indicator specifies that the fibre channel frame is encrypted;

transmitting the fibre channel frame to the second network entity.

48. (Previously Presented) An apparatus for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying a fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the fibre channel frame corresponds to the selectors of an entry in a security database;

means for encrypting a first portion of the fibre channel frame using key and algorithm information associated with the entry in the security database;

means for providing a security control indicator in the fibre channel frame, wherein the security control indicator specifies that the fibre channel frame is encrypted;

means for transmitting the fibre channel frame to the second network entity.

50. (Original) An apparatus for receiving encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying that the frame has been secured

means to lookup the security parameters in a security database that allow the de-encapsulation of the frame

means to decrypt the eventually encrypted frame

means to verify that the message has been sent by the sender, and that has not been tampered during its transmission .